Requirements

Outline

- **Operational Requirements Documents:**
  - **Initial Capabilities Document (ICD)**
  - **DOTMLPF Change Recommendation (DCR)**
  - **DOTMLPF Integrated Capabilities Recommendation (DICR)**
  - **Capability Development Document (CDD)**
  - **Capability Production Document (CPD)**
  - **Relationship with COIC and KPP**
  - **Time synchronization with COIC and TEMP**
- **Joint Capabilities Integration and Development System (JCIDS) - Requirements Determination**
- **Integrated Capabilities Development Teams (ICDTs)**
- **Critical Technical Parameters**
- **C4I Support Plan**

TEMAG T&E Refresher Course

Operational Requirements Development

I'LL DESIGN THE SYSTEM AS SOON AS YOU GIVE ME THE USER REQUIREMENTS.
BETTER YET, YOU COULD BUILD THE SYSTEM, THEN I'LL TELL YOUR BOSS THAT IT DOESN'T MEET MY NEEDS.
I DON'T MEAN TO FRIGHTEN YOU, BUT YOU'LL HAVE TO DO SOME ACTUAL WORK.
THAT'S CRAZY TALK.
www.dilbert.com scottadams@aol.com
© 2003 United Feature Syndicate, Inc.

Copyright @ 2003 United Feature Syndicate, Inc.

Definitions

Initial Capabilities Document (ICD):

- Broad, time-phased, operational goals, describe requisite capabilities
- Prepared for Concept Review
- Required for entry into Concept Refinement Phase
- Required for all program regardless of ACAT/entry point into the acquisition process
- Required for Milestone A

Capability Development Document (CDD):

- Minimum set of KPP
- Prepared by the user or user's representative
- Prepared for Milestone B - Program Initiation
- Required for entry into System Development and Demonstration Phase
- Linkage to an approved ICD unless a Capability Development Rapid Transition

Capability Production Document (CPD):

- Update/revised CDD
- Finalized after Design Readiness Review
- Required for Milestone C
- Provides authoritative, testable capabilities for Production &

TEMAC T&E Refresher Course

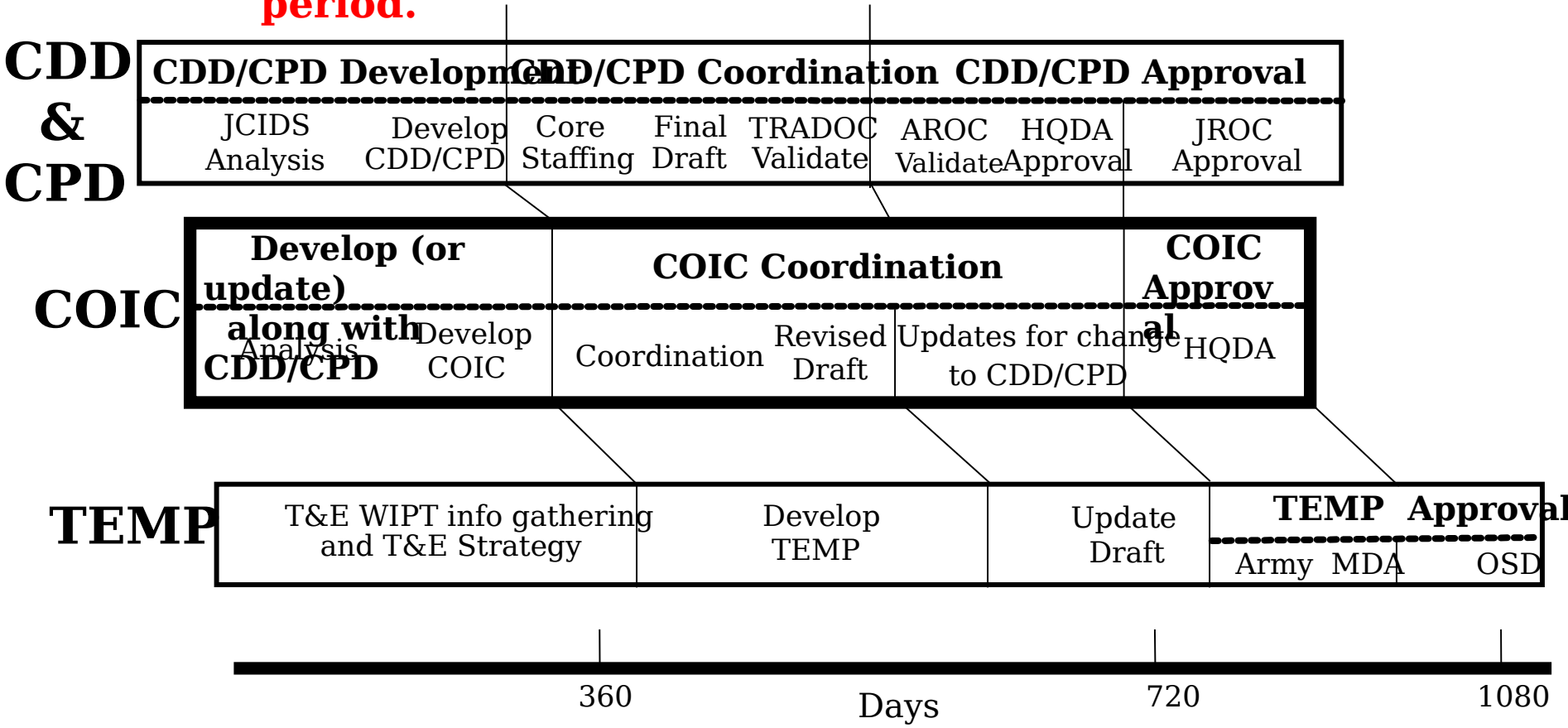
Relationships

- **Once approved, ICD normally <u>not</u> updated; CDD for MS B; CPD for MS C**
- **CDD and COIC developed together; COIC leads are:**
  - ✓ **Capability Developer for Materiel and Tactical C4/IT Programs**
  - ✓ **Force Modernization Proponent for Non-tactical C4/IT**
- **Draft COIC accompany CDD ; CDD approved before COIC approved**

KPP	COIC
Can be Show Stopper anytime (Waiver can be requested)	**Can be Show Stopper at FRP Decision Review**
Operational Requirements: **- Assessable** **- Measurable** **- Testable** **- Achievable**	**Mission oriented** **- Assessable** **- Measurable** **- Testable** **- Achievable**
Developed by ICDT	**Developed by Proponents**
Approved at MS B	**Approved by HQDA: DCS, G-8 or CIO/G-6**
Incremental Development	**Criteria include all KPP**
	Key Evaluation Measures
	Accommodate Incremental Development
	Non-major – "good enough"
	Major changes permissible until CDD approved

An Overview

NOTE: Approved CARDS # occurs by the 540-720 day period.



Capability Development Overview

- **MDA approves – authority to proceed to next phase or cancel program**
- **May not require formal Milestone A**
- **Per program and technology maturity, may enter at MS A, MS B, or MS C**
- **Entrance and Exit Criteria must be met**
- **ICD required for <u>all</u> programs plus the appropriate CDD or CPD ***
- **Change in one element of DOTMLPF may result in change in others**
- **Focus on total system-of-systems in an operational environment**

TEMAC T&E Refresher Course

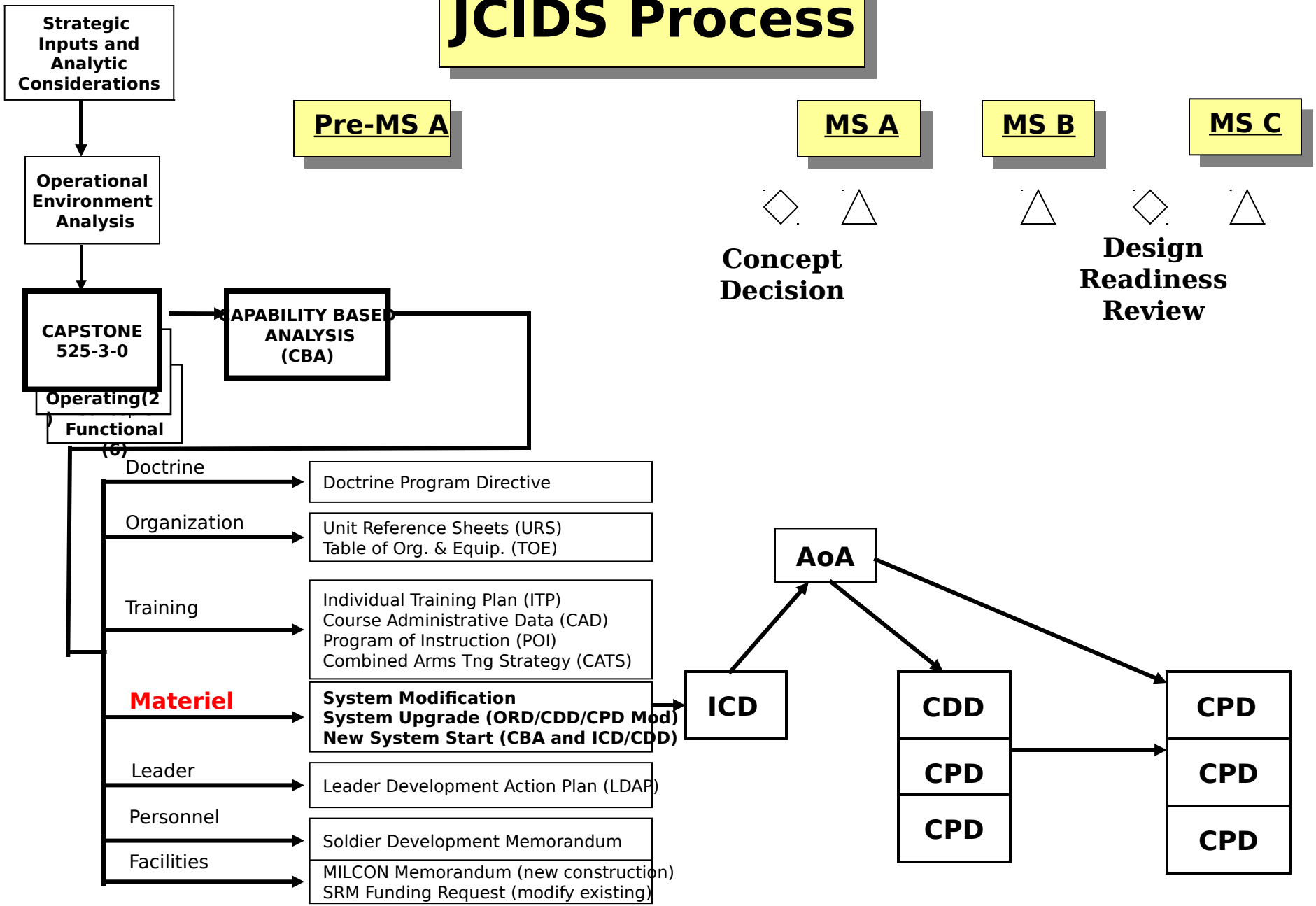
*** CDRT efforts do not require an ICD.**

Capability Documents Process

- **Developed at TRADOC Schools for Warfighting materiel / C4ISR**
- **Developed by Force Modernization Proponent for non-tactical C4 / IT programs**
- **Forwarded to HQDA G3 for AROC processing & recommendation**
- **CSA approved ***
- **Must request to initiate:**
  - **TRADOC will request HQDA to direct AoA;**
  - **HQDA provides issues for ACAT I and selected others;**
  - **TRADOC direct AoA for selected ACAT II and III;**
  - **Study Group conduct AoA**
- **TRADOC will direct schools to develop CDDs and CPDs based on the results of the functional portfolio reviews and CBAs conducted by ICDTs**
- **ICDT established – Key players CAPDEV, MATDEV,**

*** may be delegated to HQDA (DCS, G-3) or VCSA depending on ACAT and level of interest**

JCIDS Process



Integrated Capabilities Development Team (ICDT)

Definition - A managerial technique used to team all appropriate activities at one time to ensure horizontal and vertical integration of a specified capability.

Purpose - Conducts portfolio review to support ARFORGEN

cludes JCIDS Capabilities Based Assessment

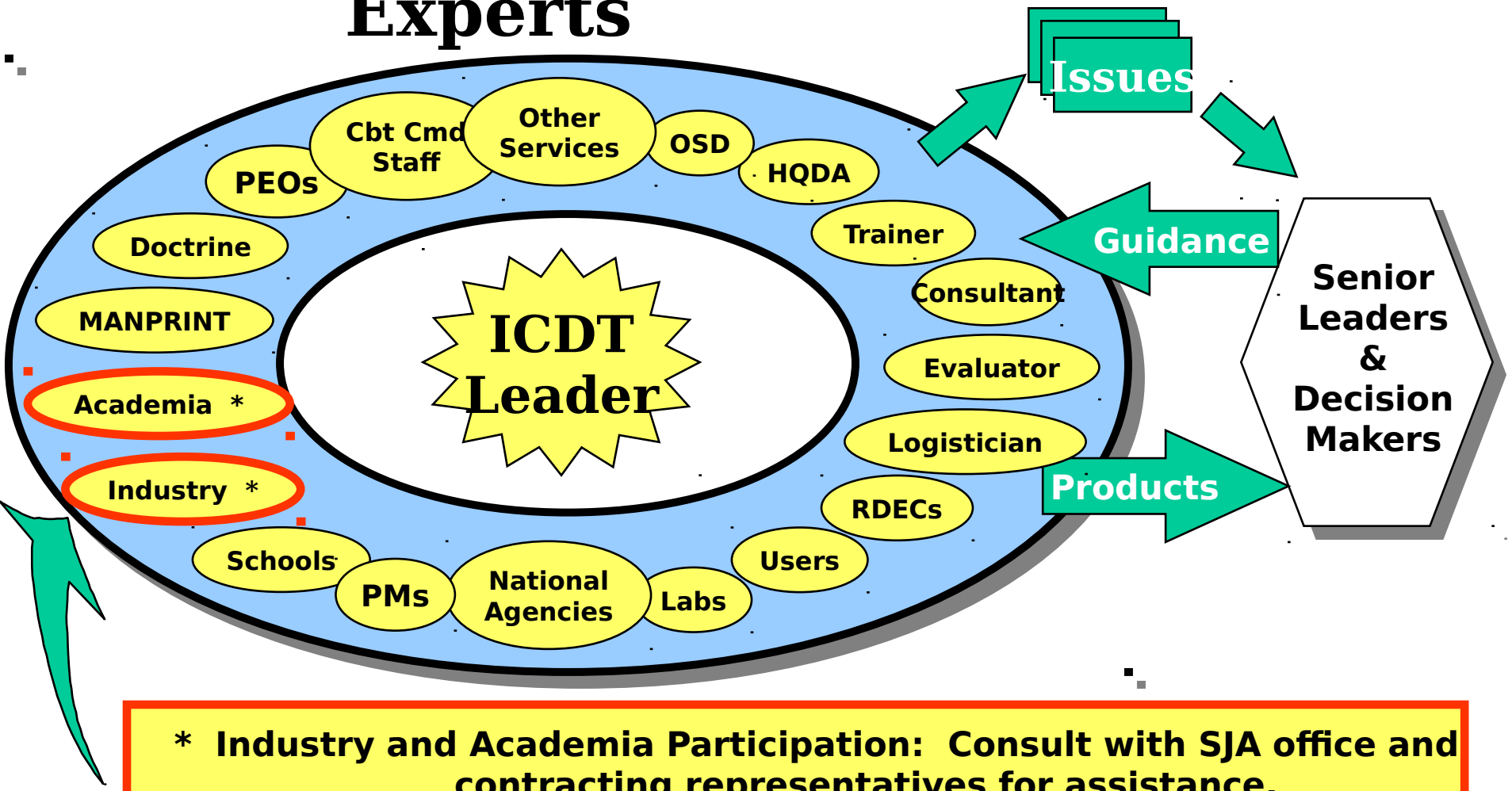
on/modification of WfE JCIDS documents and

DCR - Proposal used to document the non-materiel portion of a system or when procuring additional items of equipment.

Characteristics

- ✓ Team spirit
- ✓ **Empowered team members**
- ✓ Success oriented
- ✓ Proactive team environment
- ✓ Early issue identification
- ✓ Reasoned disagreements
- ✓ Create a "sense of ownership"
- ✓ Capitalizes on full team expertise

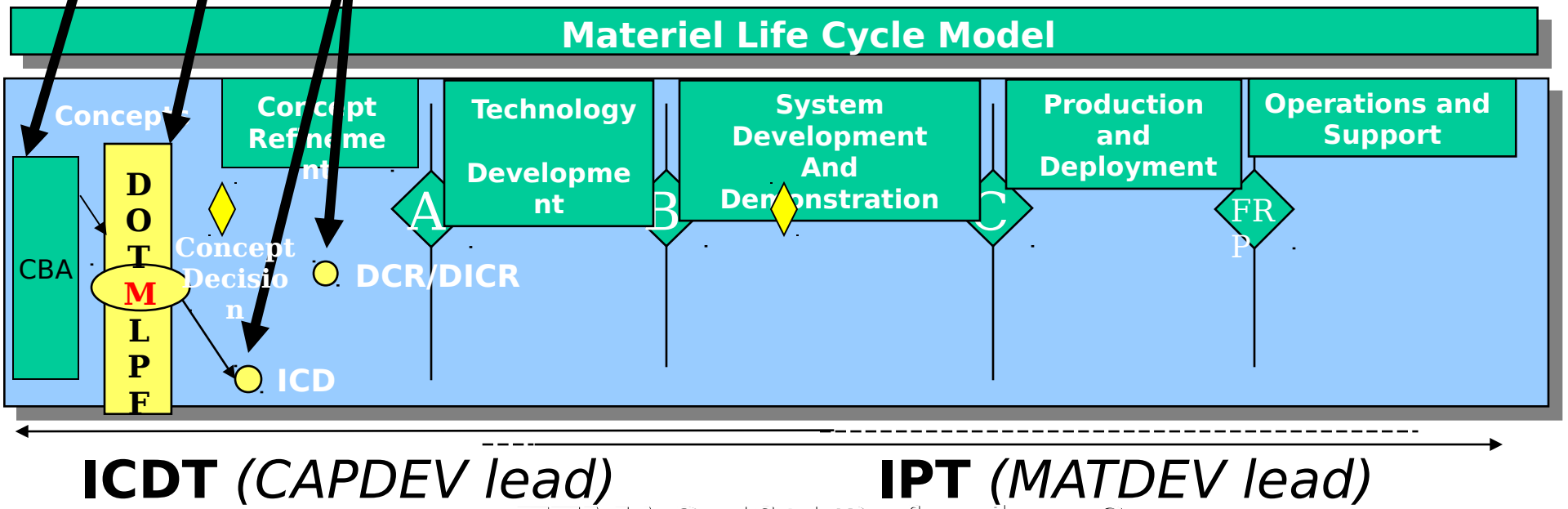
ICDT
A Flexible Team of Experts



* Industry and Academia Participation: Consult with SJA office and contracting representatives for assistance.

When ICDTs are Used?

- *When developing and conducting JCIDS analysis*
- *When determining DOTMLPF solutions*
- *When writing an ICD &/or DCR / DICR*



Critical Technical Parameters

- Technical measures of critical system characteristics ad
  - ✓ Hardware and Software maturity
  - ✓ Performance measures
- When achieved, allows the attainment of operational per requirements
- Failure to achieve is a reliable indicator that the system maturity and risk is not adequately understood and the behind in the planned development schedule
- Used to address operational test readiness certification
- Primary focus on system parameters system still needin evaluated (or reconfirmed) based upon DT

DT can often expose unknown technical risk areas.

Information Support Plan (ISP)

Mandated By:

CJCSI 6212.01E, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 15 December 2008

DoDD 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 05 May 2004

DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004

Information Support Plan (ISP)

Purpose:

MATDEV/PM Developed - Documents and Identifies Issues, Needs, Objectives and Interface Requirements of IT and NSS for;

All Acquisition Category (ACAT) Programs
Non-ACAT Programs
Fielded Programs

Provides an illustration of how a system is migrating to meet the needs of the net-centric environment

Provides a forum for the MD/PM to discuss and remedy any developmental, operational, testing or training issues that may have an adverse impact on the interoperability or supportability of a system

Value-Added:

Assists in ensuring that the acquisition community is procuring a system, or system-of-systems, that is both interoperable and supportable and has a sound integrated architecture

The ISP is a conscious transition from the development of systems based upon the requirements generation system process to the development of systems based upon joint capabilities, with a focus on net-centricity, namely, the Net-Ready Key Performance Parameter (NR-KPP)

Net-Ready Key Performance Parameter (NR-KPP)

- **Used to assess:**
  - **Information Needs**
  - **Information Timeliness**
  - **Information Assurance**
  - **Joint Interoperability & Supportability**
- **Consists of measurable/testable characteristics and performance metrics required for timely, accurate and complete exchange & use of information**
- **Desired end-result of the NR-KPP is a system with Global Information Grid Compatibility, which will define interoperability as a "many-to-many" exchange rather than a point-to-point interfaces**

Net-Ready Key Performance Parameter (NR-KPP)

- **NR-KPP Consists of:**
  - **AV-1, OV-2, OV-4, OV-5, OV-6C**
  - **SV-4, SV-5, SV-6, SV-10c (Army Required View) & TV-1 (DIS Online)**
  - **Applicable CRD Crosswalk**
  - **Initial LISI Profile**
  - **NR-KPP Statement**
  - **IA Statement of Compliance**
  - **Key Interface Profiles**

oint Interoperability Test Command's NR KPP Testing Guideboo

//www.intelink.gov/sites/jitc/nrkpp/guidebook/Wiki%20Pages/Hon

NOTE: Must register to obtain access.

Key Performance Parameters

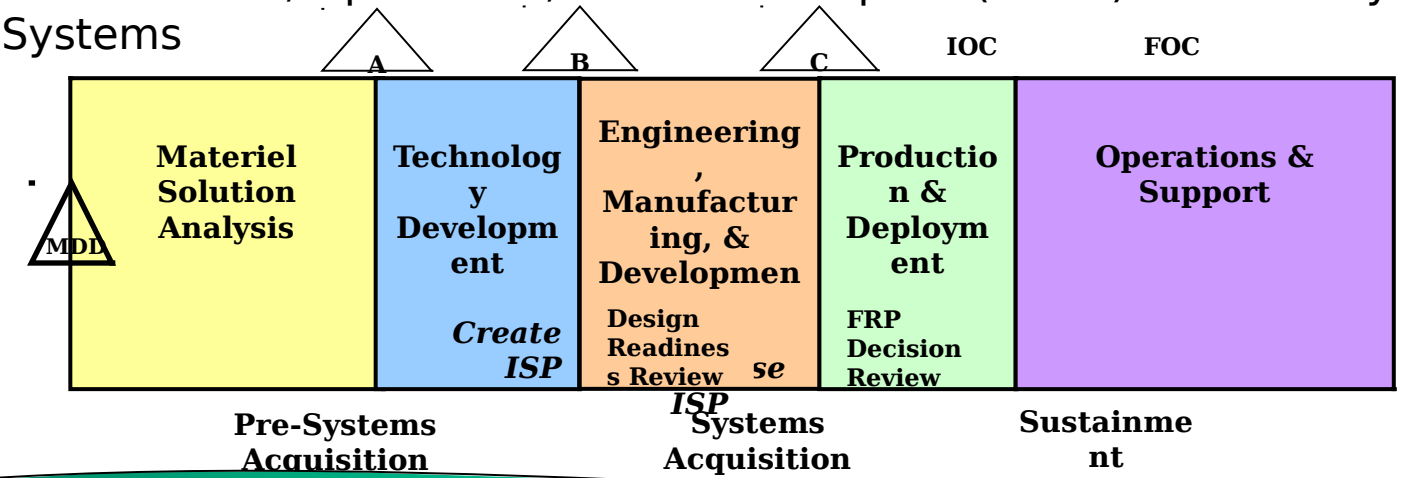
CJCSI 3170.01G
JCIDS Manual

- **Mandatory**
  - **Net-Ready**
  - **Force Protection**
  - **Survivability**
  - **Sustainment**
    - **Material Availability KPP**
    - **Material Reliability KSA**
    - **Ownership Cost KSA**

- **Selectively Applied**
  - **System Training**
  - **Energy Efficiency**

ISP Review Requirements

- ISP Review & Approval is Required at Acquisition **Milestone B, Milestone C LRIP, Major System Upgrade or Milestone Update. If Program Requirements Change subsequent to Approval at Milestone C LRIP, the ISP Must be Reviewed & Approved at Milestone C FRP.**
- Army ISP Approval Authority is US Army CIO/G-6 Director of Architectures, Operations, Networks & Space (AONS) for All Army Systems



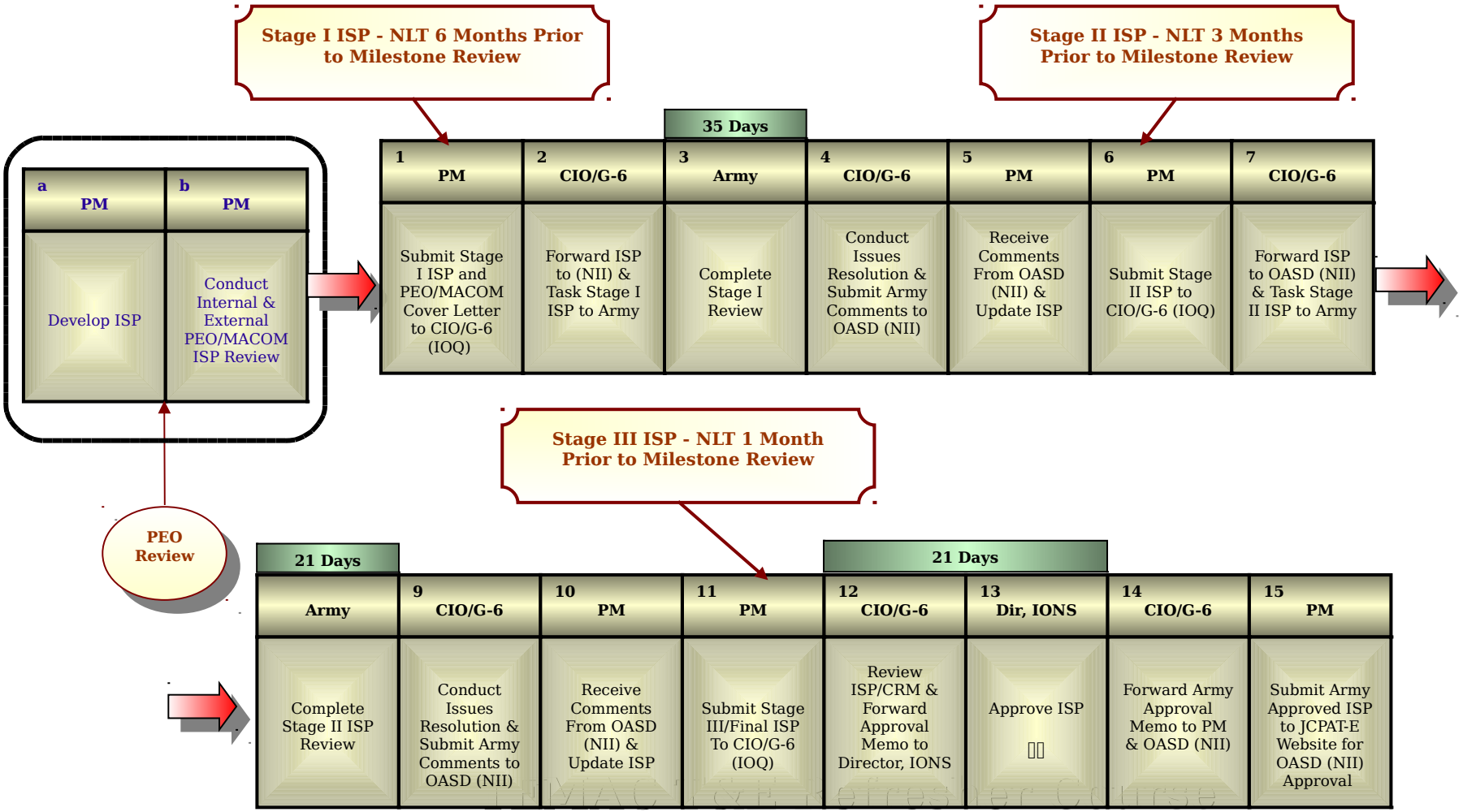
gram or system ISPs, regardless of MDA, must be approved by HQDA, CIO/G-6, Dir.,

U.S. Army ISP Review Process

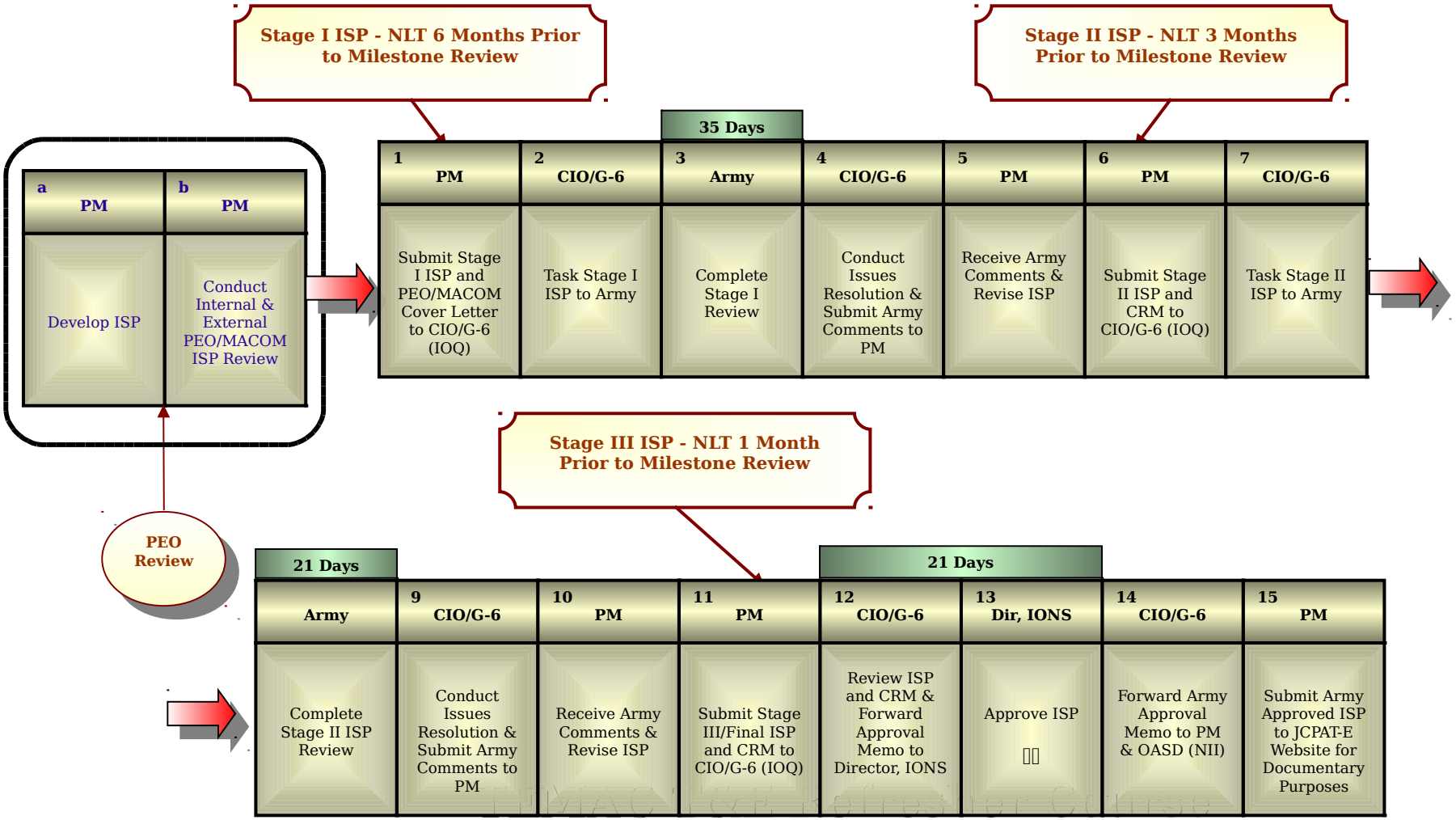
Four Stage Review Process:

Pre-Stage I
PM Conduct Internal/External Review of Document
Provide PEO/MACOM Signed Cover Letter to US Army CIO/G-6
Stage I
35 day review cycle
Staffed to DoD, DA, PEO & MACOM Communities
Reviewed at the O-6/GS-15 Level
Upon completion, comments forwarded to PM for document revision
Stage II
21 day review cycle
Staffed to DoD, DA, PEO & MACOM Communities
Reviewed at the GO/SES Level
Upon completion, comments forwarded to PM for document revision
Stage III
Ensure all Stage II comments are responded to
Forward approval memo to US Army CIO/G-6 Dir., AONS for signature
Approval memo forwarded to OASD (NII) & PM

Review Process – ACAT I / OSD


Stage I ISP - NLT 6 Months Prior to Milestone Review
Stage II ISP - NLT 3 Months Prior to Milestone Review
35 Days
a PM
Develop ISP
b PM
Conduct Internal & External PEO/MACOM ISP Review
1 PM
Submit Stage I ISP and PEO/MACOM Cover Letter to CIO/G-6 (IOQ)
2 CIO/G-6
Forward ISP to (NII) & Task Stage I ISP to Army
3 Army
Complete Stage I Review
4 CIO/G-6
Conduct Issues Resolution & Submit Army Comments to OASD (NII)
5 PM
Receive Comments From OASD (NII) & Update ISP
6 PM
Submit Stage II ISP to CIO/G-6 (IOQ)
7 CIO/G-6
Forward ISP to OASD (NII) & Task Stage II ISP to Army
PEO Review
Stage III ISP - NLT 1 Month Prior to Milestone Review
21 Days
21 Days
Army
Complete Stage II ISP Review
9 CIO/G-6
Conduct Issues Resolution & Submit Army Comments to OASD (NII)
10 PM
Receive Comments From OASD (NII) & Update ISP
11 PM
Submit Stage III/Final ISP To CIO/G-6 (IOQ)
12 CIO/G-6
Review ISP/CRM & Forward Approval Memo to Director, IONS
13 Dir, IONS
Approve ISP
14 CIO/G-6
Forward Army Approval Memo to PM & OASD (NII)
15 PM
Submit Army Approved ISP to JCPAT-E Website for OASD (NII) Approval

Review Process – ACAT II & Below


Stage I ISP - NLT 6 Months Prior to Milestone Review
Stage II ISP - NLT 3 Months Prior to Milestone Review
35 Days
a PM
Develop ISP
b PM
Conduct Internal & External PEO/MACOM ISP Review
1 PM
Submit Stage I ISP and PEO/MACOM Cover Letter to CIO/G-6 (IOQ)
2 CIO/G-6
Task Stage I ISP to Army
3 Army
Complete Stage I Review
4 CIO/G-6
Conduct Issues Resolution & Submit Army Comments to PM
5 PM
Receive Army Comments & Revise ISP
6 PM
Submit Stage II ISP and CRM to CIO/G-6 (IOQ)
7 CIO/G-6
Task Stage II ISP to Army
PEO Review
Stage III ISP - NLT 1 Month Prior to Milestone Review
21 Days
21 Days
Army
Complete Stage II ISP Review
9 CIO/G-6
Conduct Issues Resolution & Submit Army Comments to PM
10 PM
Receive Army Comments & Revise ISP
11 PM
Submit Stage III/Final ISP and CRM to CIO/G-6 (IOQ)
12 CIO/G-6
Review ISP and CRM & Forward Approval Memo to Director, IONS
13 Dir, IONS
Approve ISP
14 CIO/G-6
Forward Army Approval Memo to PM & OASD (NII)
15 PM
Submit Army Approved ISP to JCPAT-E Website for Documentary Purposes

Acknowledgement & Feedback

This module is a part of the T&E Managers Committee (TEMAC) T&E Refresher Course.

Request your feedback. Please contact -

T&E Office
Deputy Under Secretary of the Army
102 Army Pentagon
Washington, D.C. 20310-0102
(703) 602-3508 / 2134 DSN: 332